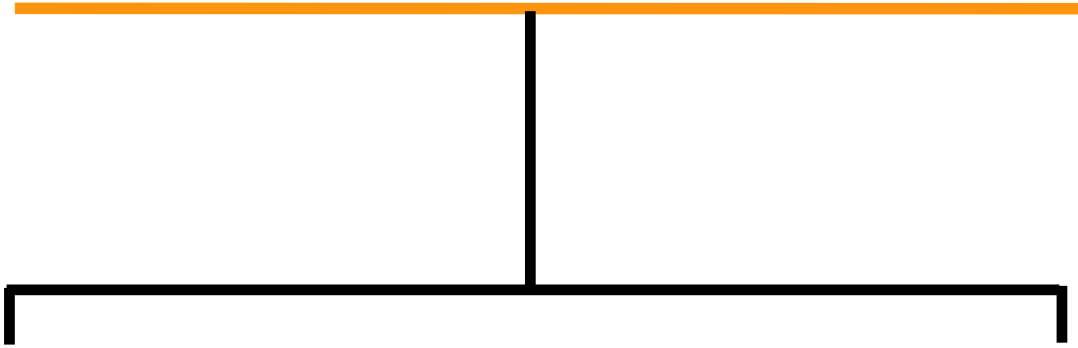
Cryptography Review

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 5-Crypto Review

ravi.utsa@gmail.com
www.profsandhu.com

Cryptographic Technology



SYMMETRIC KEY

Secret Key
Single Key
Conventional

ASYMMETRIC KEY

Public Key
Public-Private Key

Cryptographic Technology

- Symmetric-key encryption
- Symmetric-key message authentication codes (MAC)
- Public-key encryption
- Public-key digital signatures
- Message digests (hash functions)

SSL uses all of these

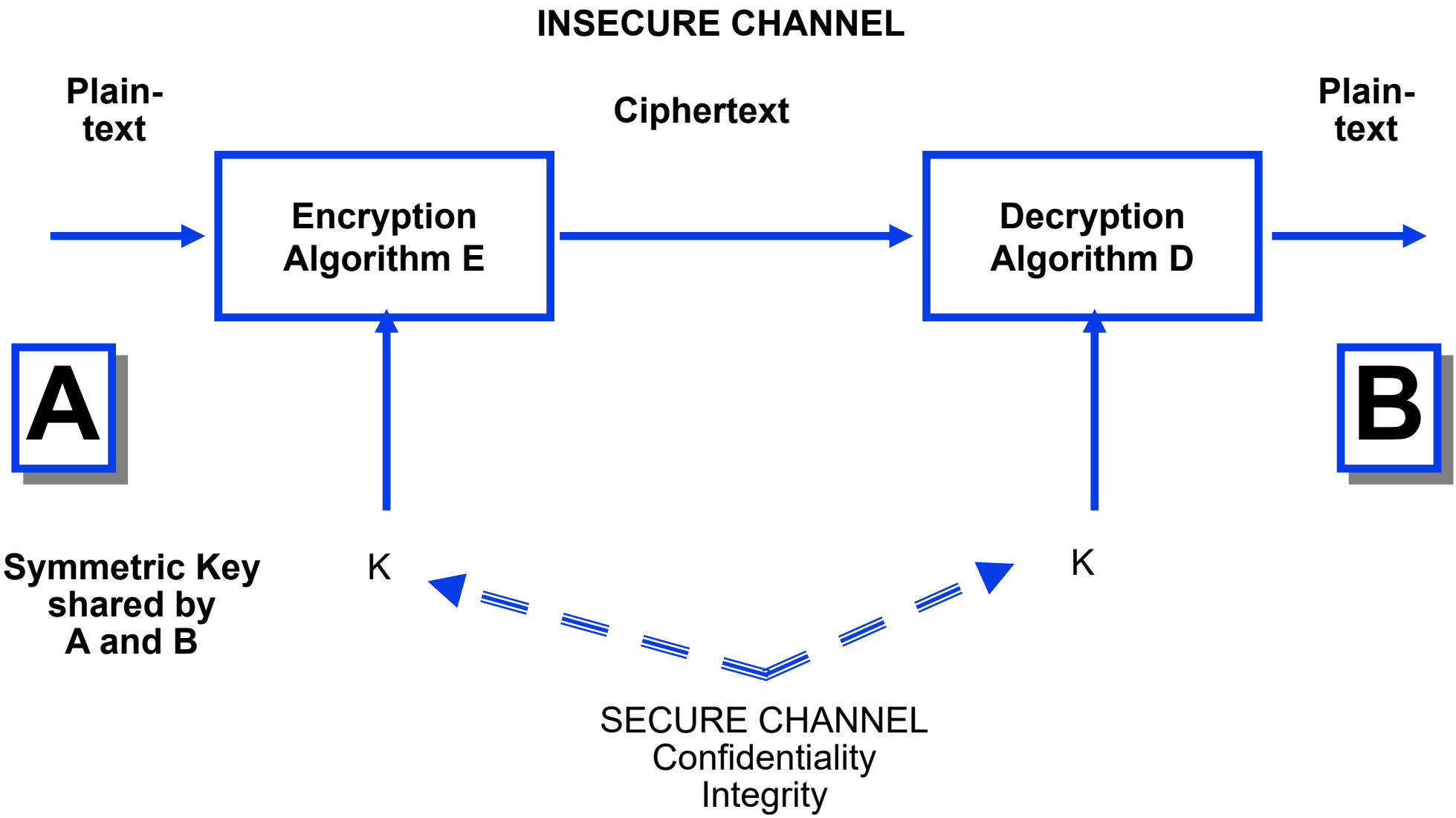
- Public-key certificates
- Public-key key agreement
- Challenge-response authentication
- Replay protection

ATMs run on symmetric-key technology

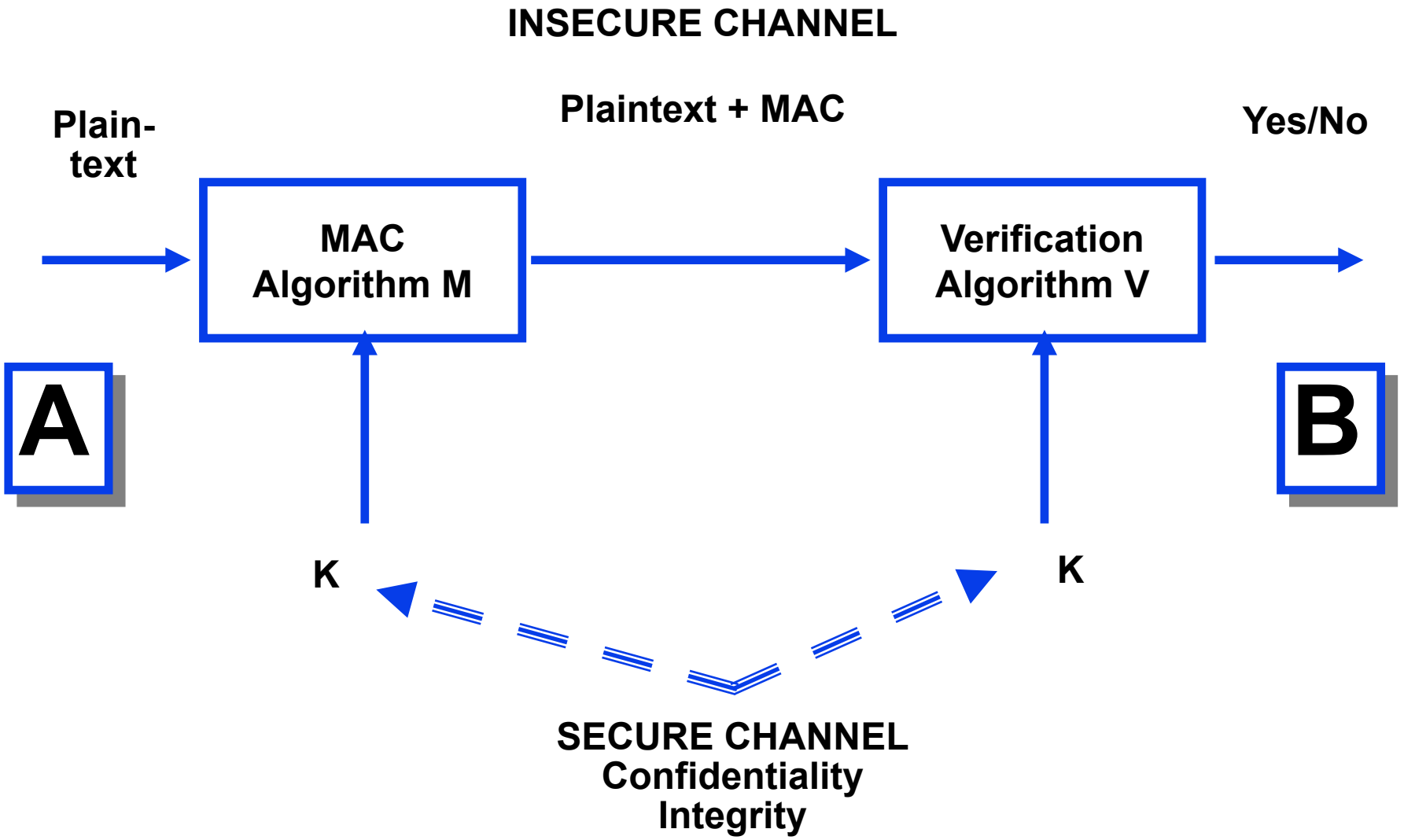
Cryptographic Services

- confidentiality
  - crypto keys leak profusely via side channels
- integrity + authentication
  - no point having one without the other
- non-repudiation
  - requires asymmetric cryptography
  - stronger form of integrity + authentication

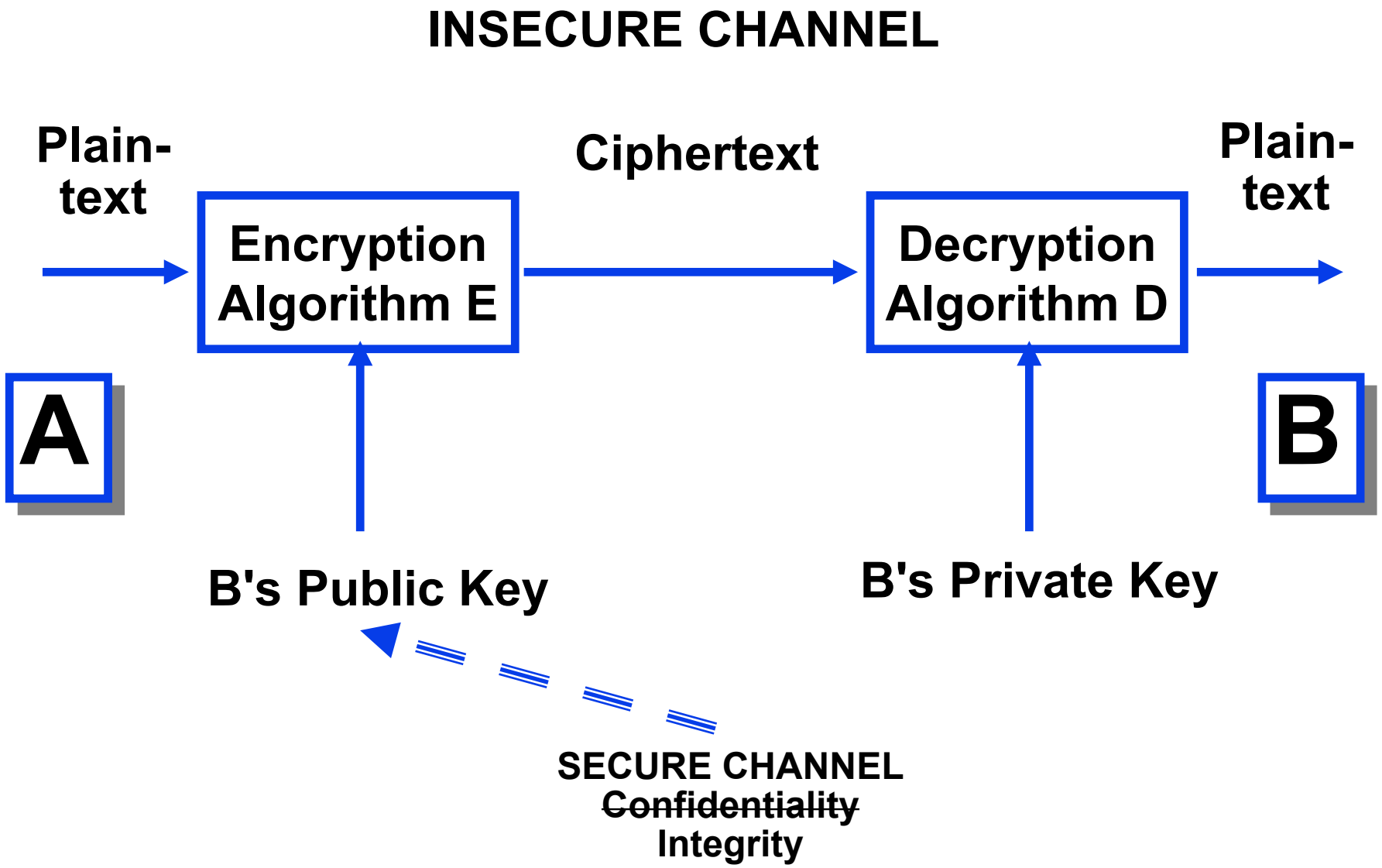
Symmetric-Key Encryption



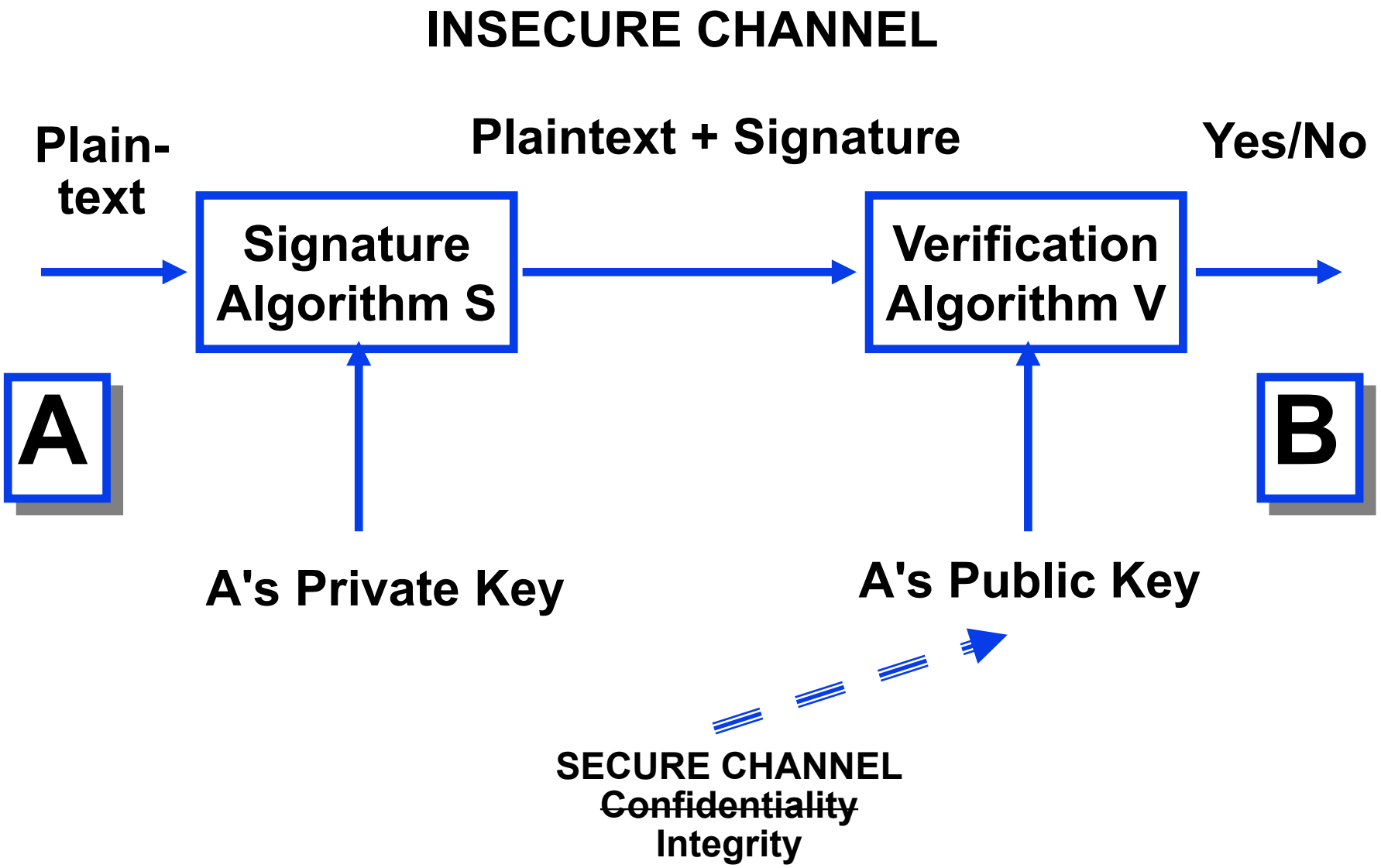
Symmetric Key Message Authentication Code



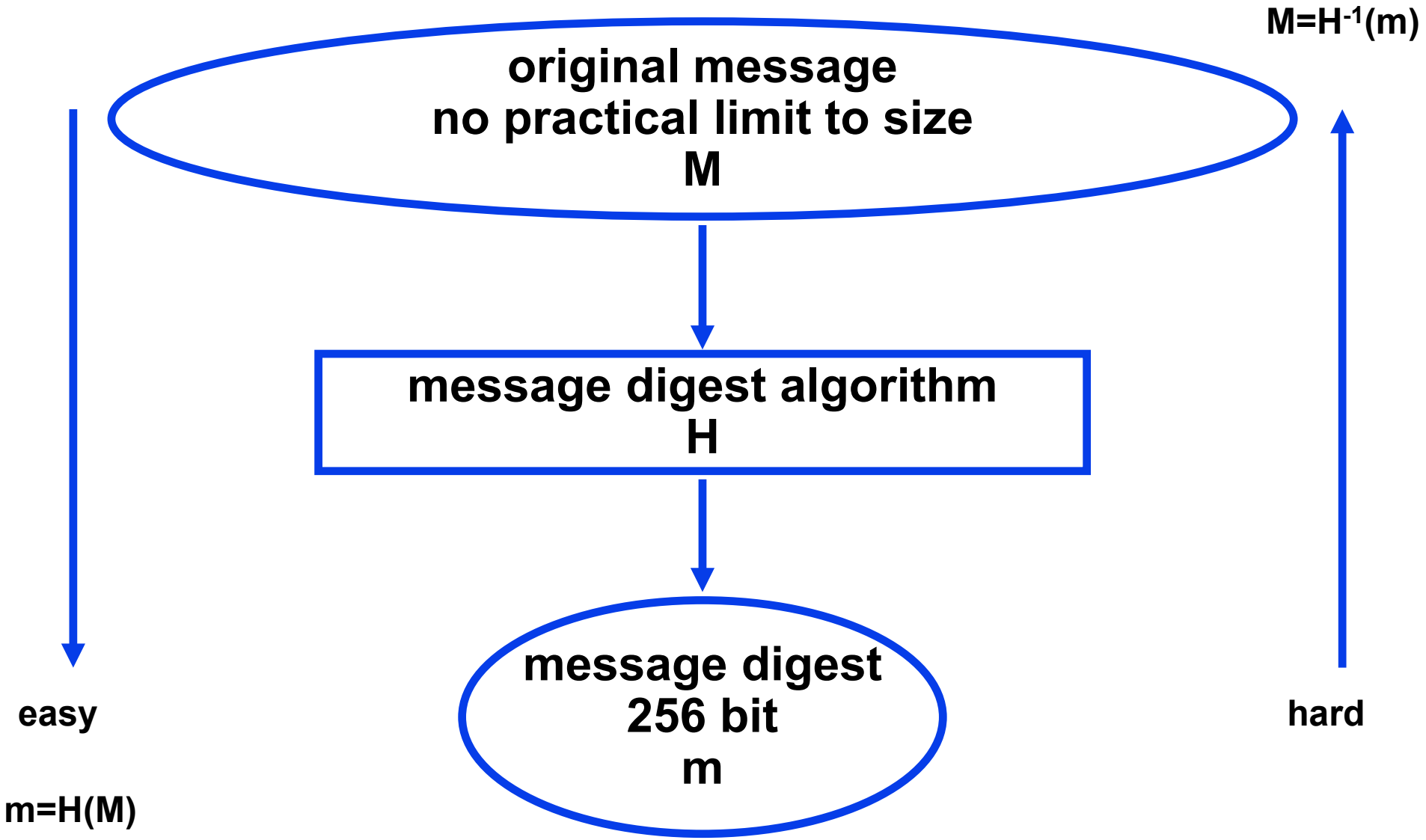
Public-Key Encryption



Public-Key Digital Signature



Message Digest (Hash)



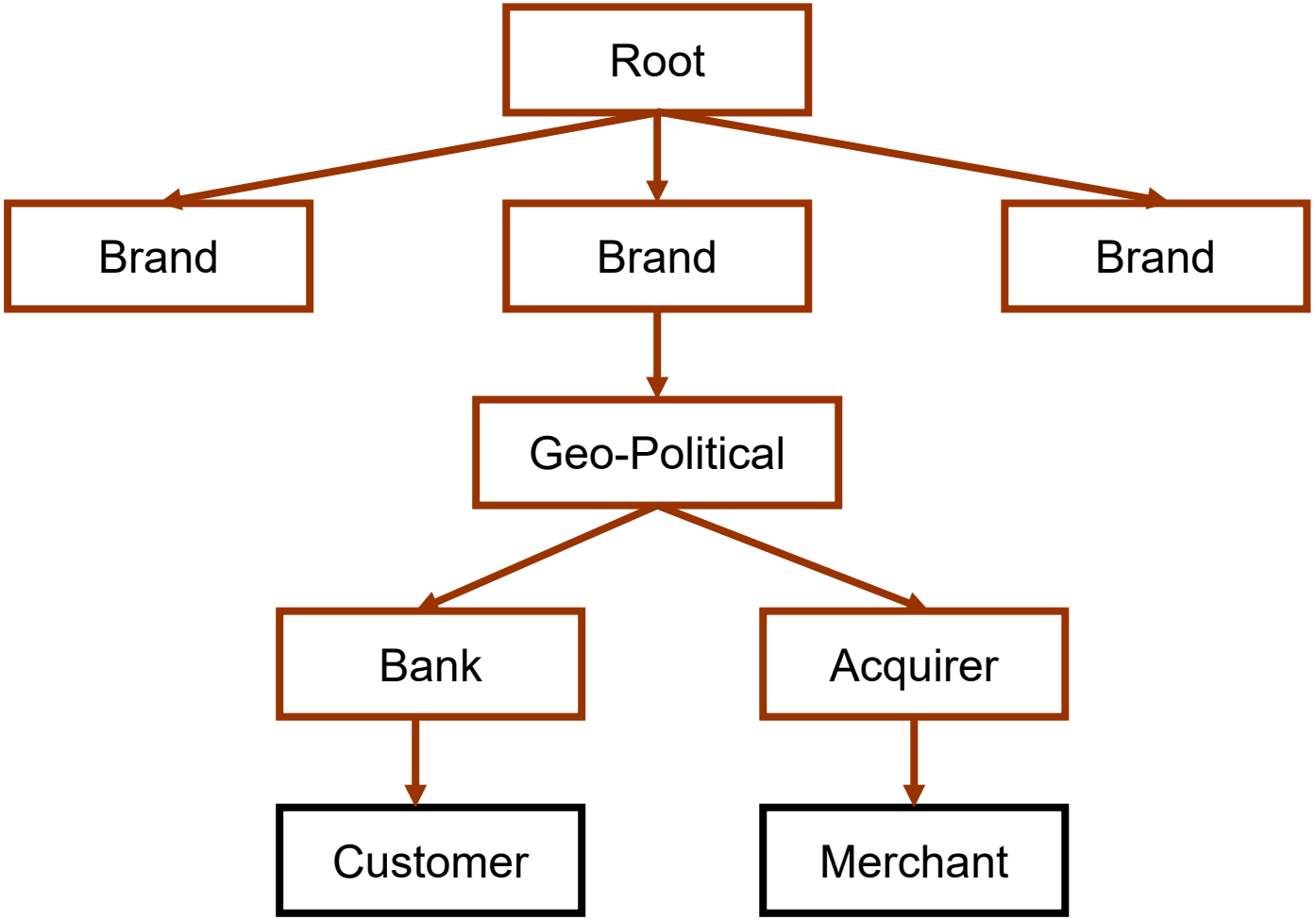
X.509v1 Certificate

VERSION
SERIAL NUMBER
SIGNATURE ALGORITHM
ISSUER (Certificate Authority)
VALIDITY
SUBJECT
SUBJECT PUBLIC KEY INFO
SIGNATURE

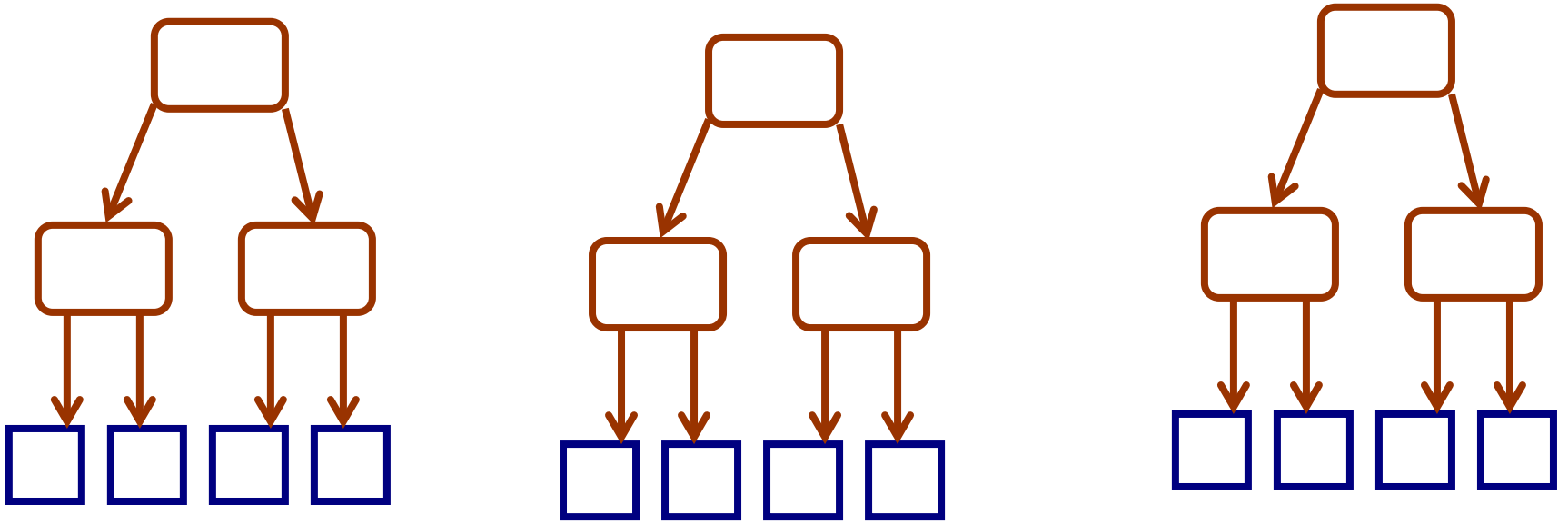
X.509v1 Certificate

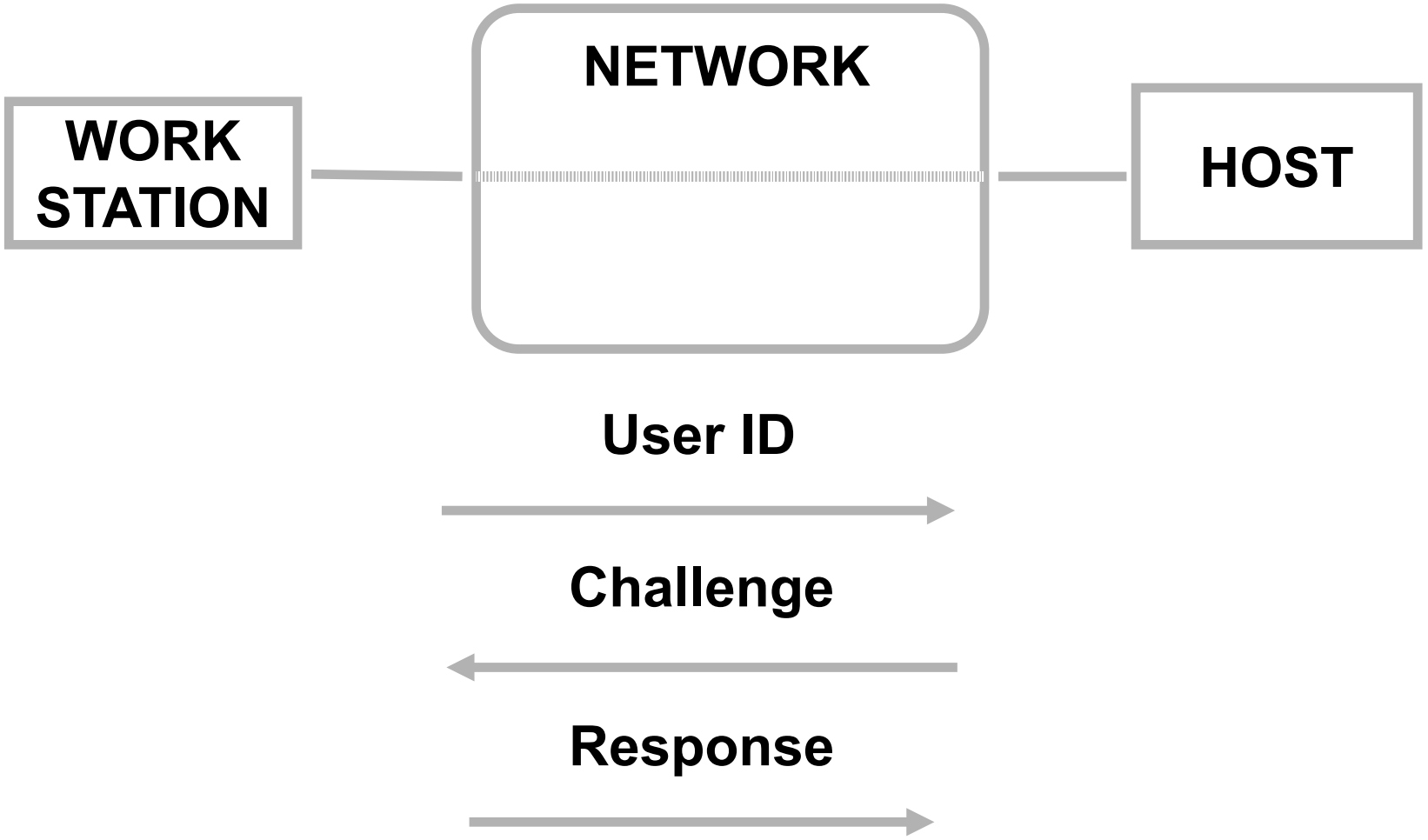
1
12345678910111213 14
RSA+SHA-3, 2048
C=US, S=VA, O=GMU, OU=ISE
1/1/19-12/31/20
C=US, S=TX, O=UTSA, OU=CS, CN=Ravi Sandhu
RSA, 2048, xxxxxxxxxxxxxxxxxxxxxxxxx
SIGNATURE

SET CA Hierarchy



Multiple Trusted Roots



© Ravi Sandhu

Challenge-Response Authentication